Несимметричные крипто-кодовые конструкции Мак-Элиса и Нидеррайтера в постквантовой криптографии

УДК 004.056.55

Алексей Цыганенко[1], Сергей Евсеев[2], Карина Мельник[3]

[1,2]Харьковский национальный экономический университет им. С. Кузнеца, [3]Национальный технический университет «Харьковский политехнический институт», [1]oleksii.tsyhanenko@hneu.net, [2]serhii.yevseiev@hneu.net, [3]karina.v.melnyk@gmail.com

Быстрый рост объемов обрабатываемых данных и развитие вычислительной техники выдвигают новые требования к обеспечению надежности и безопасности данных. Наиболее часто используемыми алгоритмами обмена ключами в TLS являются алгоритмы RSA, Диффи-Хелмана и Диффи-Хелмана на эллиптических кривых. Эти алгоритмы, соответственно, зависят от целочисленной проблемы факторизации, задачи Диффи-Хелмана и задачи эллиптической кривой. И пока неизвестны алгоритмы для решения этих задач в полиномиальное время, данные алгоритмы обмена ключами являются криптостойкими. Однако, проведенные исследования в области влияния квантовых вычислений, использующих явления квантовой суперпозиции и квантовой запутанности для передачи и обработки данных, показали, что квантовые компьютеры, смогут решить упомянутые задачи в полиномиальное время используя алгоритм Шора.

Практически вся используемая асимметричная криптография может быть эффективно нарушена квантовыми алгоритмами. С другой стороны, симметричная криптография, похоже, способна пережить атаки квантовых компьютеров. Лучшие квантовые атаки на симметричные шифры и хеш-функции, известные в настоящее время, используют алгоритм Гровера. Чтобы найти 256-битный симметричный ключ из нескольких открытых текстов и зашифрованных текстов или для получения прообраза для 256-битной хэш-функции, алгоритму Гровера требуется приблизительно 2128 итераций. На практике также могут быть значительные накладные расходы из квантовой коррекции ошибок. Хотя мощные квантовые компьютеры еще не существуют, ожидается, что это будет только вопрос времени, прежде чем они смогут использоваться для разрыва текущих алгоритмов обмена ключами.

В феврале 2016 года NIST опубликовал отчет о пост-квантовой криптографии, в котором говорится, что многие ученые теперь считают, что создание большого квантового компьютера является важной технической задачей, хотя все же необходимы существенные долгосрочные усилия для фактического построить квантовый компьютер. NIST неохотно дает конкретные оценки того, когда будут доступны масштабные квантовые компьютеры. Приблизительная оценка: «вероятно, что квантовый компьютер способен разлома RSA-2048 в течение нескольких часов может быть построено к 2030 году при бюджете около миллиарда долларов». Квантовые компьютеры уже успешно факторизуют малые целые числа. Фактом для беспокойства является то, что злоумышленник может хранить перехваченные ключевые обмены и зашифрованные тексты сегодня и расшифровывать их,

когда будет доступен крупномасштабный квантовый компьютер. В зависимости от того, когда (и если) станут доступными мощные квантовые компьютеры, это может сделать текущую асимметричную криптографию непригодной для шифрования долгосрочных секретов.

Известен ряд средств защиты от квантовых компьютерных атак. Возможным решением является использование распределения квантовых ключей, которое использует квантовую связь для обмена ключа между двумя сторонами. Безопасность такого решения может быть математически доказана, если придерживаться некоторых физических законов. Существенным недостатком этого решения является несовместимость с текущим сетевым оборудованием. Другим решением является использование классических криптосистем, которые, как известно, не уязвимы для квантовых компьютерных атак, например, используя только симметричную криптографию. Третьим и наиболее перспективным решением является замена уязвимой асимметричной криптографии криптосистемами, которые по-прежнему считаются защищенными в квантовом мире.

В уже упомянутом отчете NIST, одними из алгоритмов, которые считаются устойчивыми к атакам как классическим так и квантовым, названы криптосистемы Мак-Элиса и Нидеррайтера. Это постквантовые криптосистемы с открытым ключом, опубликованная в 1978 году Робертом Мак-Элисом. Их безопасность основана на проблеме декодирования линейных кодов. Если код неотличим от случайного линейного кода, это NP-полная задача. Хотя это не означает жесткости для среднего случая или даже для конкретных кодов (многие специальные коды были нарушены структурными атаками), они по-прежнему дает уверенность в том, что эти криптосистемы не будут нарушены общими атаками. Мак-Элис является одной из старейших криптосистем с открытым ключом и имеет функции быстрого шифрования и дешифрования. Криптосистема Нидеррайтера является вариантом криптосистемы Мак-Элиса, опубликованным в 1986 году. С точки зрения безопасности вариант Нидеррайтера эквивалентен оригинальной криптосистеме Мак-Элиса. Он называется двойным вариантом Мак-Элиса, потому что он использует матрицу проверки на четность вместо матрицы генератора, а зашифрованные тексты состоят из синдромов, а не кодовых слов, к которым добавлен вектор ошибки. Преимущество этого варианта заключается в том, что открытый ключ немного меньше. Для двоичного линейного кода длины n, ранга k и минимального расстояния d матрица открытого ключа имеет размеры $(n-k) \times n$ вместо $k \times n$ для Мак-Элиса. Использование криптосистемы Нидеррайтера для шифрования и дешифрования несколько медленнее, чем криптосистемы Мак-Элиса, потому что сообщения должны быть закодированы в векторы ошибок.

Подводя итог можно сказать, что поскольку упомянутые конструкции являются уверенными кандидатами для постквантовой криптографии, исследование их модификаций, с целью снижения энергозатрат криптопреобразований и повышения криптостойкости, является перспективным направлением.